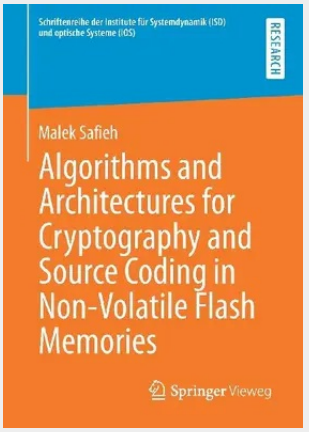
Safieh

Algorithms and Architectures for Cryptography and Source Coding in Non-Volatile Flash Memories



In this work, algorithms and architectures for cryptography and source coding are developed, which are suitable for many resource-constrained embedded systems such as non-volatile flash memories. A new concept for elliptic curve cryptography is presented, which uses an arithmetic over Gaussian integers. Gaussian integers are a subset of the complex numbers with integers as real and imaginary parts. Ordinary modular arithmetic over Gaussian integers is computational expensive. To reduce the complexity, a new arithmetic based on the Montgomery reduction is presented. For the elliptic curve point multiplication, this arithmetic over Gaussian integers improves the computational efficiency, the resistance against side channel attacks, and reduces the memory requirements. Furthermore, an efficient variant of the Lempel-Ziv-Welch (LZW) algorithm for universal lossless data compression is investigated. Instead of one LZW dictionary, this algorithm applies several dictionaries to speed up the encoding process. Two dictionary partitioning techniques are introduced that improve the compression rate and reduce the memory size of this parallel dictionary LZW algorithm.

In this work, algorithms and architectures for cryptography and source coding are developed, which are suitable for many resource-constrained embedded systems such as non-volatile flash memories. A new concept for elliptic curve cryptography is presented, which uses an arithmetic over Gaussian integers. Gaussian integers are a subset of the complex numbers with integers as real and imaginary parts. Ordinary modular arithmetic over Gaussian integers is computational expensive. To reduce the complexity, a new arithmetic based on the Montgomery reduction is presented. For the elliptic curve point multiplication, this arithmetic over Gaussian integers improves the computational efficiency, the resistance against side channel attacks, and reduces the memory requirements. Furthermore, an efficient variant of the Lempel-Ziv-Welch (LZW) algorithm for universal lossless data compression is investigated. Instead of one LZW dictionary, this algorithm applies several dictionaries to speed up the encoding process. Two dictionary partitioning techniques are introduced that improve the compression rate and reduce the memory size of this parallel dictionary LZW algorithm.

53,49 €
49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783658344580
Medium: Buch
ISBN: 978-3-658-34458-0
Verlag: Springer
Erscheinungstermin: 11.08.2021
Sprache(n): Englisch
Auflage: 1. Auflage 2021
Serie: Schriftenreihe der Institute für Systemdynamik (ISD) und optische Systeme (IOS)
Produktform: Kartoniert
Gewicht: 216 g
Seiten: 142
Format (B x H): 148 x 210 mm